REMARKS

Favorable reconsideration of this application, in light of the preceding amendments and following remarks, is respectfully requested.

Claims 17-35 are currently pending in this application, of which claim 17 is the sole independent claim and the remainder dependent. Claim 17 is currently amended.

DISCUSSION OF EXAMPLE EMBODIMENTS

A non-limiting example embodiment is described to assist the Examiner in understanding the function of the present application and the differences between the present application and the prior art references. Applicants submit that this description is only to assist the Examiner's understanding and should not limit any of claims 17-35 in any way. Instead, each claim should be interpreted solely based upon the limitations presented therein.

According to a non-limiting example embodiment, the security module 10 and the receiver 11 are jointly denominated the devices. The security module 10 may be, for example, in the form of a microchip card or a module including a chip. The security module 10 may contain a private asymmetric key PAKV of a pair of asymmetric keys. **This key may be introduced into the security module 10, for example, at the time the module is manufactured or at a later stage, in a managing data centre or by a secure connection between said managing centre and the security module**. The private asymmetric key PAKV may be stored in a non-volatile memory of the module. (Emphasis Added)

According to a non-limiting example embodiment, the receiver 11 may be a box connected to a television set. It may contain a public asymmetric key PAKB from the pair of asymmetric keys. This public key may be matched to the private key of the security module. **The public key PAKB may also be programmed**

during the manufacture of the receiver or during an initialization phase in a protected environment. It may also be safely remotely loaded by broadcasting. (Emphasis Added)

Rejections under 35 U.S.C. § 103

Claims 17-35 stand rejected under 35 U.S.C. § 103(a) as being anticipated by EP 0 537 971 B1 to Hardy et al. ("Hardy") in view of WO 00/30319 to Kupka et al. ("Kupka") and further in view of U.S. Patent No. 6,507,907 to Takahashi et al. ("Takahashi"). Applicants respectfully traverse this rejection for the reasons detailed below.

It is alleged in the Office Action at pages 4-5 that Hardy teaches a traffic key (allegedly, the "session key" of claim 17, as per the Examiner) to encrypt and decrypt the data exchanged between terminal A and terminal B in FIG. 3 of Hardy.

However, the traffic key of Hardy is not used by terminal A and terminal B for any data exchange. At most, Hardy teaches exchanging traffic keys via a public key or another method. See, Hardy, col. 8, lines 11-12. Absent any such teachings, Applicants submit that Hardy fails to teach or fairly suggest "using the session key to encrypt and decrypt all or part of the exchanged data between the first and second device," as required by claim 17. Also, in Hardy, the communication is between multiple receivers situated remotely. Similarly, Kupka also involves remote communication between a broadcast center and a receiver.

Acknowledging the deficiencies of Hardy in teachings each and every limitation of claim 17, the Examiner relies on the teachings of Kupka and Takahashi to cure the noted deficiencies of Hardy. Specifically, the Examiner alleges that Kupka discloses "the first encrypting key initialized in the first device during an initialization phase of the first device in a first protected environment," as recited in claim 17 and Takahashi discloses "the second encrypting key

initialized in the second device during an initialization phase of the second device in a second protected environment," as recited in claim 17.

In Kupka, user information and vendor information (allegedly the "first encrypting key" of claim 17 as per the Examiner) is temporarily stored in a RAM 64. However, the RAM 64 does not offer any protected environment. Further, none of the storing of the user information and vendor information and any generation of the compound encryption/decryption key is carried out "during an initialization phase of the first device." For at least these reasons, Kupka fails to teach or fairly suggest "the first encrypting key initialized in the first device during an initialization phase of the first device in a first protected environment," as recited in claim 17.

In Takahashi, a trusted third party supplies corresponding secret keys. However, Takahashi fails to disclose or even suggest any "protected environment" as required by claim 17, let alone initialization of the secret keys in a protected environment. For at least these reasons, Takahashi fails to teach or fairly suggest "the second encrypting key initialized in the second device during an initialization phase of the second device in a second protected environment," as recited in claim 17.

Absent any such teachings, Applicants submit that Kupka and Takahashi fail to overcome the noted deficiencies of Hardy. Therefore, the alleged combination of Hardy, Kupka and Takahashi also fails to render the limitations of claim 17 obvious to one of ordinary skills in the art. Claims 18-35, dependent on independent claim 17, are patentable for the reasons stated above with respect to claim 17 as well as for their own merits.

Applicants, therefore, respectfully request that the rejection to claims 17-35 under 35 U.S.C. § 103 be withdrawn.

CONCLUSION

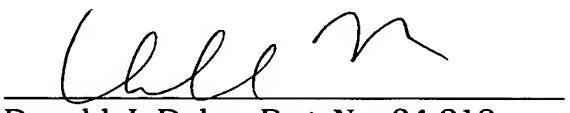
In view of the above remarks and amendments, the Applicants respectfully submit that each of the pending rejections has been addressed and overcome, placing the present application in condition for allowance. A notice to that effect is respectfully requested. If the Examiner believes that personal communication will expedite prosecution of this application, the Examiner is invited to contact the undersigned.

Should there be any outstanding matters that need to be resolved in the present application, the Examiner is respectfully requested to contact Donald J. Daley at the telephone number of the undersigned below.

If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 08-0750 for any additional fees required under 37 C.F.R. § 1.16 or under 37 C.F.R. § 1.17; particularly, extension of time fees.

Respectfully submitted,

HARNESS, DICKEY, & PIERCE, P.L.C.

By 

Donald J. Daley, Reg. No. 34,313
P.O. Box 8910
Reston, Virginia 20195
(703) 668-8000

DJD/AZP:cfc